The University of Alberta
Printing Department
Edmonton, Alberta

THE UNIVERSITY OF ALBERTA

RELEASE FORM

NAME OF AUTHOR: BRIAN CHARLES MORTIMER

TITLE OF THESIS: PRIMITIVE PERMUTATION GROUPS OF PRIME POWER DEGREE

DEGREE FOR WHICH THESIS WAS PRESENTED M.Sc.

YEAR THIS DEGREE GRANTED 1975

Permission is hereby granted to THE UNIVERSITY OF ALBERTA LIBRARY to reproduce single copies of this thesis and to lend or sell such copies for private, scholarly or scientific research purposes only.

The author reserves other publication rights, and neither the thesis nor extensive extracts from it may be printed or otherwise reproduced without the author's written permission.

THE UNIVERSITY OF ALBERTA

PRIMITIVE PERMUTATION GROUPS OF PRIME POWER DEGREE

by

© BRIAN MORTIMER

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES AND RESEARCH

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE

OF MASTER OF SCIENCE

IN

MATHEMATICS

DEPARTMENT OF MATHEMATICS

EDMONTON, ALBERTA

FALL, 1975

THE UNIVERSITY OF ALBERTA

FACULTY OF GRADUATE STUDIES AND RESEARCH

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies and Research, for acceptance, a thesis entitled PRIMITIVE PERMUTATION GROUPS OF PRIME POWER DEGREE submitted by BRIAN MORTIMER in partial fulfillment of the requirements for the degree of Master of Science in Mathematics.

DEDICATION

To *Campanula lasiocarpa* and the other treasures of the high, windblown and solitary places.

ABSTRACT

In 1969, H. Wielandt [12] developed a new method for studying permutation groups by using the algebra of functions mapping the permuted set into a field. Using this technique he was able to classify the uni-primitive groups of degree p^2 .

In this thesis we apply the Wielandt method to the case of degree p^3 . Chapter III is devoted to generalizing these techniques to more than two variables and to general results on primitivity. Chapter IV contains the main theorems. It is shown there (Theorem 4.1) that a uni-primitive group of degree p^3 containing a regular elementary abelian subgroup is either contained in the affine group, "almost" imprimitive or else very non-geometric. Finally, the last two possibilities are eliminated when $p = 3$ (Theorem 4.6).

ACKNOWLEDGEMENT

I would like to thank R.D.Bercov for suggesting the topic and reading the final draft, and Graham Chambers for reading the primeval editions with such good humour during a beautiful June when he had much better things to do. Also I would like to thank Graham and Frank Markel for listening so patiently when I needed to be listened to.

Finally,I want to express my appreciation to the National Research Council of Canada for their continuing love,affection and support.

TABLE OF CONTENTS

CHAPTER I

Introduction

Let $V(n,p^e)$ denote the n - dimensional vector space over the field, $\mathbb{F}_{p^e}$, with p^e elements; $V(n,p^e)$ has p^{en} vectors. In this vector space we call the translates of the linear vector subspaces, linear sub-varieties. It is sometimes conceptually advantageous to neglect completely the co-ordinate system of $V(n,p^e)$ and concentrate only on the incidence relationships of the linear sub-varieties. The result is the affine n - space over $\mathbb{F}_{p^e}$, denoted $AG(n,p^e)$.

The automorphism group of $AG(n,p^e)$ consists of all collineations of $AG(n,p^e)$, i.e. all mappings of the points to the points which map linear sub-varieties to linear sub-varieties. In terms of the vector space structure we can realize this group as the set of all mappings $x \mapsto Ax^\alpha + b$ where $A \in GL(n,p^e)$, the general linear group; x, b in $V(n,p^e)$ and $\alpha \in Aut(\mathbb{F}_{p^e})$ acts on x componentwise (Artin [2]). We denote this group by $Aff(n,p^e)$ and call it the affine group. From the form of the mappings in $Aff(n,p^e)$ given above we easily deduce the order of the group from the order of $GL(n,p^e)$ and $Aut(\mathbb{F}_{p^e})$.

Lemma 1.1: The order of $Aff(n,p^e)$ is $e \cdot p^{\frac{ne(n+1)}{2}} \cdot \prod_{i=1}^{n} (p^{ei}-1)$.

We see that $Aff(n,p^e)$ and its subgroups provide many examples of permutation groups of degree a power of p. Note that since $GL(n,p^e)$ is transitive on the non-zero vectors of $V(n,p^e)$, $Aff(n,p^e)$ is a 2-transitive permutation group; it is not in general 3-transitive. So we might hope to find many permutation groups of

degree p^m for some m which are not multiply transitive among the subgroups of $Aff(n,p^e)$ where $m = ne$.

In fact we can restrict ourselves to $Aff(m,p)$. For if $m = en$ then $V(m,p)$ is isomorphic as an $\mathbb{F}_p$ - vector-space to $V(n,p^e)$. Also an $\mathbb{F}_{p^e}$ - linear transformation on $V(n,p^e)$ is also $\mathbb{F}_p$ - linear and corresponds under the above isomorphism to an $\mathbb{F}_p$ - linear transformation on $V(m,p)$. Moreover since any $\alpha \in Aut(F_{p^e})$ fixes $\mathbb{F}_p$ elementwise, the automorphisms of $\mathbb{F}_{p^e}$, induce $\mathbb{F}_p$ - linear transformations on $V(n,p^e)$ and hence on $V(m,p)$. Therefore we may consider $Aff(n,p^e)$ as a permutation subgroup of $Aff(m,p)$ whenever $m = ne$.

We make the following definition:

Definition: Let G permute Ω transitively. If whenever we have a $\Delta \subseteq \Omega$ such that $\forall\, g \in G$, $\Delta^g \cap \Delta = \Delta$ or ϕ, we have $\Delta = \Omega$ or $|\Delta| = 1$ then we say that G is primitive.

Lemma 1.2: G is primitive if and only if the subgroup $G_\alpha = \{g \in G \mid \alpha^g = \alpha\}$ is maximal in G.

Proof: See Wielandt [11; pg. 15].

Every multiply transitive group is primitive, but there are primitive groups which are not 2-transitive and we call such a group uni-primitive.

In 1906 Burnside [5, pg. 339] proved the following result:

Theorem 1.3: Let G be a transitive permutation group of degree p. Let P be a Sylow p - subgroup of G. Then either

(i) $P \lhd G$, $G \leq \mathrm{Aff}(1,p)$ and $|P| = p$, or

(ii) G is 2 - transitive.

In 1969 Wielandt [12] was able to show that a corresponding result holds for p^2;

Theorem 1.4: Let G be a transitive permutation group of degree p^2, and let P be a Sylow p - subgroup of G then either

(i) G is uni-primitive, P is regular elementary abelian of order p^2 and

(a) $P \lhd G$, $G \leq \mathrm{Aff}(2,p)$, or

(b) $G \rhd N$, N an imprimitive subgroup of index 2, or

(ii) G is imprimitive, or

(iii) G is 2 - transitive.

In this thesis, we consider the case of degree p^3. Many results are proved, though, for the case of p^n. This work is essentially a generalization of the latter sections of Wielandt [12] and many results from this source are assumed here without proof.

CHAPTER II

The Sylow p - Subgroup of G

In the case of degree p^1 and, with more difficulty, in the case of degree p^2 we can prove that when G is uni-primitive, a Sylow p - subgroup, P, of G is a regular elementary abelian subgroup. This allows us to represent P as the translations in a finite vector space and G as a permutation group of this vector space. The following example shows that we can not hope for a general result of this type in the case of degree p^3.

2.1 Example: The Group of the 27 Lines on a Cubic Surface.

A general cubic surface in complex three space contains exactly 27 straight lines. These are positioned in such a way that each is concurrent with 10 others. The resulting incidence structure has an automorphism group with an index 2 subgroup G of order 25,920. This latter group, G is abstractly isomorphic with several classical groups including $PSp(4,3)$ and $PSU(4,2)$ and is simple. There have been a number of extensive studies made of this group and its associated incidence structures, for example Baker [4], Dickson [5].

G has a 5 dimensional complex representation. In fact $G = \langle B,C,D,S \rangle$ where, (Baker [4]; pg. 61)

$$B = \frac{1}{\sqrt{-3}} \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & \omega & \omega^2 \\ 0 & 0 & 1 & \omega^2 & \omega \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix},$$

$$D = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \omega^2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \omega^2 & 0 \\ 0 & 0 & 0 & 0 & \omega^2 \end{pmatrix}$$

and ω is a primitive cube root of unity. Note that $B^4 = C^3 = D^2 = S^3 = 1$. Now let $E = (DS^2)^2$, $T = C^{-1}EC$, $U = ES$. Then $U^3 = E^3 = T^3 = 1$ and,

$$E = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \omega & 0 & 0 & 0 \\ 0 & 0 & \omega & 0 & 0 \\ 0 & 0 & 0 & \omega^2 & 0 \\ 0 & 0 & 0 & 0 & \omega^2 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \omega & 0 & 0 & 0 \\ 0 & 0 & \omega^2 & 0 & 0 \\ 0 & 0 & 0 & \omega & 0 \\ 0 & 0 & 0 & 0 & \omega^2 \end{pmatrix}, \quad U = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & \omega & 0 & 0 \\ 0 & 0 & 0 & \omega & 0 \\ 0 & 0 & 0 & 0 & \omega \end{pmatrix}.$$

Thus $L = \langle E,U,T \rangle$ is an elementary abelian group of order 27. C acts on L by, $U^C = U$, $E^C = T$, $T^C = U^{-1}E^{-1}T^{-1}$. Thus $C \in N_G(L)$ and $H = \langle E,U,T,C \rangle$ is a sub-group of G of order 81. As $25{,}920 = 2^6 \cdot 3^4 \cdot 5$, H is Sylow.

Since H is a non-abelian p-group, $9 \leq [H:Z(H)] \leq 27$. If $[H : Z(H)] = 9$ then since $C_L(\langle C \rangle) = \langle U \rangle$, $\exists F \in Z(H) \setminus L$. But then $H = \langle F,L \rangle$ is abelian which is not the case. Thus $[H : Z(H)] = 27$ and $Z(H) = \langle U \rangle$.

Now consider $K = \langle B,D,E,(DC^2)^2 \rangle$. This is a maximal sub-group of G of order $960 = 2^6 \cdot 3 \cdot 5$, Baker [3, pg. 71], Dickson [7, pg. 305]. Thus K has index 27 in G and G acting on K by conjugation

gives a primitive action of degree 27. Note that since $26 \nmid |G|$, G is not 2 - transitive in this action. Thus G provides an example of a degree p^3 uni-primitive group in which the Sylow p - subgroup has order $p^4 > p^3$.

Moreover G does not contain any regular abelian subgroups. For if L' was one such then by a suitable conjugation, since L' is a 3 - group, $L' < H$. Now $L' \cap K = \langle 1 \rangle$ so $L' \not\trianglelefteq L$. Therefore $H = LL'$ and $|L \cap L'| = 9$. But then $L \cap L'$ commutes with both L and L' and hence with H . But Z(H) has order 3. Therefore G contains no regular abelian subgroups.

G does in fact contain a regular subgroup. Indeed C normalizes the subgroup $\langle U, ET^{-1} \rangle$ of L , so that $L' = \langle U, ET^{-1}, C \rangle$ is of order 27. Furthermore, $K \cap L' = K \cap H \cap L' = \langle E \rangle \cap L' = \langle 1 \rangle$. Therefore $G = K \cdot L'$ and L' is transitive of order 27, i.e. it is regular.

We observe finally that as $o(G) = 2^6 \cdot 3^4 \cdot 5$ and $o(\mathrm{Aff}(3,3)) = 2^6 \cdot 3^5 \cdot 13$, G is not a subgroup of Aff(3,3) .

It would be interesting to know if there are uni-primitive groups of degree p^n without regular subgroups.

2.2 Remarks on the Sylow p - Subgroups of G .

The above example shows that we must modify our assumptions, in the p^3 case, if we are to distinguish uni-primitive subgroups of the affine group. We therefore make the following assumption.

Assumption: G is a permutation group acting on Ω, a set of order p^n, and G contains a regular elementary abelian subgroup, T.

We can identify Ω with $V(n,p)$ in such a way that T becomes the translations. Now, $T \lhd \mathrm{Aff}(n,p)$. Conversely if g is any permutation of Ω such that $T^g = T$, then in particular g permutes the maximal subgroups of T amongst themselves. This implies that g permutes the orbits of the maximal subgroups and so takes hyperplanes to hyperplanes. Thus $g \in \mathrm{Aff}(n,p)$.

Theorem 2.1: $G \cap \mathrm{Aff}(n,p) = N_G(T)$.

We can make a few general remarks about the Sylow p - subgroup of G.

Lemma 2.2: If T is not Sylow then

(i) $p \mid [N_G(T) : T]$, and

(ii) $|Z(P)| \leq p^{n-1}$ for any Sylow p - subgroup P of G.

Proof:

(i) Let P be a Sylow p - subgroup containing T. Then $T \neq P$ so $T \leq_+ N_P(T) \leq N_G(T)$ since P is a p - group. Therefore $p \mid [N_P(T) : T] \mid [N_G(T) : T]$.

(ii) As above $C_G(T)$ consists of collineations, but T is self-centralizing in $\mathrm{Aff}(n,p)$ since it is a regular normal subgroup. Therefore $Z(P) \leq T$. But since $Z(P) \leq T \leq_+ P$, P does not centralize T and $Z(P) < T$. □

CHAPTER III

Techniques and Tools

3.1 The Function Space:

In [12], Wielandt has developed a method for detailed study of a permutation group acting on a set Ω, which involves looking at the vector space of functions $f : \Omega \to K$ for some field K.

Definition: For a field K, let $F_1 = \{f : \Omega \to K\}$. If emphasis is needed on the field, we write $F_1[K]$.

F_1 is an algebra under pointwise multiplication and addition of functions. In the case that Ω is a vector space of dimension n we can use Lagrange interpolation and represent any function on Ω by a polynomial in n variables. If $\Omega = V(n,p)$ then the function X_i^p is the same as X_i so that two distinct polynomials may represent the same function. This means that we can not quite manipulate the elements of F_1 as polynomials unless the degrees stay small. For any polynomial f, we let $[f]$ denote its reduction to lowest degrees using $X_i^p = X_i$ for each i.

Many of the standard tools of analysis can be applied to these finite function spaces. We make the following definitions:

Definitions: (i) For any subset Δ of Ω let χ_Δ be the characteristic function of Δ i.e. $\chi_\Delta(\rho) = 0$ if $\rho \notin \Delta$, $= 1$ if $\rho \in \Delta$.

(ii) For $f = \sum a_{e_1 \ldots e_n} X_1^{e_1} \ldots X_n^{e_n} \in F_1$ define the partial

derivative of f with respect to X_i by

$$\frac{\partial f}{\partial X_i} = \sum e_i \, a_{e_1 \ldots e_n} X_1^{e_1} \ldots X_i^{e_i - 1} \ldots X_n^{e_n} \quad .$$

(iii) For $f \in F_1$, and, for each subset Δ of Ω, define the integral of f over Δ by $\int_\Delta f = \sum_{\rho \in \Delta} f(\rho)$.

(iv) For $f, g \in F_1$ define the convolution of f and g by $(f*g)(\rho) = \int_\Omega f(\omega) g(\rho - \omega) \, d\omega$.

(v) For $f \in F_1$, $f = \sum a_{e_1, \ldots, e_n} X_1^{e_1} \ldots X_n^{e_n}$, let deg $f = \max \{e_1 + \ldots + e_n : a_{e_1 \ldots e_n} \neq 0\}$, the degree of f $(e_i \leq p-1 \ , \ \forall i)$.

(vi) For a subset M of F_1, let deg $M = \max\{\deg f : f \in M\}$.

Note that definitions (ii), (v) and (vi) are contingent on Ω being a vector space.

We generalize some of the technical results of Wielandt [12] to n variables, in the following sections.

3.1.1 Integration.

We assume that F_1 is a ring of polynomials over a field and that Ω is a vector space over $\mathbb{F}_p$. It is straightforward from the definition that integration is a linear functional. Thus we may integrate term by term. Moreover

$$\int_\Omega X_1^{e_1} \dots X_n^{e_n} = \int_{\mathbb{F}_p} X_1^{e_1} \int_{\mathbb{F}_p} X_2^{e_2} \dots \int_{\mathbb{F}_p} X_n^{e_n} ,$$

so it is enough to evaluate $\int_{\mathbb{F}_p} X^m$ for all choices of m. But this is just $1 + 2^m + \dots + (p-1)^m \pmod p$. Let $I_m = \int_{\mathbb{F}_p} X^m = \sum_{a=1}^{p-1} a^m$. Then if $b \neq 0$, $I_m = \sum a^m = \sum (ba)^m = b^m I_m$. Thus $(b^m-1)I_m = 0$ and $I_m = 0$ unless $b^m = 1$ for all $b \neq 0$. In $\mathbb{F}_p$, $b^m = 1$ for every b only if $m = p-1$. Then $I_{p-1} = (p-1)\cdot 1 = -1$. Therefore,

$$\int_\Omega X_1^{e_1} \dots X_n^{e_n} = \begin{cases} 0 & \text{if } \exists_i \ e_i \neq p-1 \\ (-1)^n & \text{if } \forall_i \ e_i = p-1 \end{cases} .$$

It follows that if $f = \sum a_{e_1 \dots e_n} X_1^{e_1} \dots X_n^{e_n}$, with all $e_i \leq p-1$, then $\int_\Omega f = (-1)^n a_{p-1,\dots,p-1}$ and $\int_\Omega f = 0$ if and only if $\deg f < n(p-1)$. We can say more. If $\pi = a_1X_1 + \dots + a_n X_n + b$ then $\pi = 0$ is the equation of a hyperplane. We will let π stand, ambiguously, for both the hyperplane and its equation. Since $a^{p-1} = 1$ for all $a \neq 0$ in $\mathbb{F}_p$, $\chi_\pi = (1-\pi^{p-1})$. Now a d - dimensional linear subvariety, γ, of $\Omega = AG(n,p)$ is the intersection, $\pi_1 \cap \dots \cap \pi_d$, of some set of d hyperplanes. And $\chi_\gamma = \chi_{\pi_1} \cdot \dots \cdot \chi_{\pi_d}$ so $\deg \chi_\gamma \leq d(p-1)$.

Theorem 3.1: If $f \in F_1$ and $\deg f < (n-d)(p-1)$ then $\int_\gamma f = 0$ for every d - dimensional linear sub-variety, γ, of Ω.

Proof: $\int_\gamma f = \int_\Omega f \ \chi_\gamma$ and $\deg f \chi_\gamma < n(p-1)$. □

3.1.2 Differentiation.

All of the usual differentiation properties hold except the chain and product formulae. In these latter cases problems arise due to the cancellation phenomena. However we will not have to differentiate any products in this work with total degree greater than $p-1$ and in this situation differentiation of products by the product formula is valid.

Let $D = \alpha_1 \frac{\partial}{\partial x_1} + \ldots + \alpha_n \frac{\partial}{\partial x_n}$ and π be a hyperplane, $\pi = a_1 x_1 + a_n x_n$. Then $D(\pi) = \sum \alpha_i a_i = 0$ if and only if $(\alpha_1,\ldots,\alpha_n)$ is a point of the hyperplane. Thus given two hyperplanes π_1, π_2 through $(0,0,\ldots,0)$, we can find linear differential operators D_1, D_2 such that $D_1(\pi_1) \neq 0 = D_1(\pi_2)$ and $D_2(\pi_1) = 0 = D_2(\pi_2)$. By similar arguments we can show that if γ is a subspace of Ω then D annihilates χ_γ if and only if $(\alpha_1,\ldots,\alpha_n) \in \gamma$.

3.1.3 Convolution.

Convolutions arise naturally in the study of the functions $f : \Omega \to K$ for the following reason. If T is the translations on Ω and KT is the group algebra of T over K then there is an additive isomorphism $\phi : F_1 \to KT$ given by $\phi(f) = \sum_{t \in T} f(\theta^t) \cdot t$ where we fix once and for all $\theta = (0,0,\ldots,0)$ in Ω. Now if we use the group algebra multiplication to define, via the bijection ϕ, a new multiplication on F_1, we obtain the convolution product. Thus $\langle F_1,+,* \rangle \simeq \langle KT,+,\cdot \rangle$.

The following result relates the degrees of the convolutes to the degrees of their convolution product.

Theorem 3.2: If Ω is the n - dimensional vector space over $\mathbb{F}_p$ and $f_i \in F_1$ (hence reduced) and if $\deg f_1 + \deg f_2 = m$, then

(i) $m < n(p-1) \Rightarrow f_1 * f_2 = 0$

(ii) $m \geq n(p-1) \Rightarrow \deg f_1 * f_2 \leq \deg f_1 + \deg f_2 - n(p-1)$

(iii) $m \geq (2n-1)(p-1) \Rightarrow \deg f_1 * f_2 = \deg f_1 + \deg f_2 - n(p-1)$.

Proof: As in Wielandt [12, pg. 78, lemma 17.10] we only have to show that the terms of highest degree in the product $f_1 * f_2$ of (iii), don't cancel.

If $\deg f_i = n_i$ then among the terms of f_i of degree n_i, choose the maximal exponent e_1^i of X_1. Then amongst those terms of degree n_i containing $X_1^{e_1^i}$, choose the maximal exponent of X_2, e_2^i. Repeat this process with each variable in succession.

Claim: $X_1^{e_1^1} \dots X_n^{e_n^1} * X_1^{e_n^2} \dots X_n^{e_n^2} \neq 0$. First $e_1^i + \dots + e_n^i = n_i$ and $n_1 + n_2 \geq (2n-1)(p-1)$. Thus, since $e_j^1 + e_j^2 \leq 2(p-1)$ for every j, we must have $e_j^1 + e_j^2 \geq p-1$ for each j. Then as in Wielandt [12, pg. 78], the convolution is not zero.

Claim: the term $X_1^{e_1^1+e_1^2-(p-1)} \dots X_n^{e_n^1+e_n^2-(p-1)}$ coming from the above convolution, comes from no other convolution of monomials in f_1 and f_2. For if $X_1^{d_1^1} \dots X_n^{d_n^2} * X_1^{d_1^2} \dots X_n^{d_n^2}$ gives this term then $d_j^1 + d_j^2 = e_j^1 + e_j^2$ for all j. If $n_i > d_1^i + \dots + d_n^i$ for either i then $n_1+n_2 = e_1^1 + \dots + e_n^1 + e_1^2 + \dots + e_n^2 > d_1^1 + \dots + d_n^1 + d_n^2 + \dots + d_n^2$, a contradiction. Therefore the terms

of the product are of degree n_1 and n_2 respectively. Now we use the maximality of the e_j^i's for successive j's to show that $d_j^i = e_j^i$ for all i and j . □

3.2 G - Modules and Primitivity.

G is a permutation group acting on Ω and F_1 consists of functions mapping Ω to a field K . To relate the two objects we must define a G action on F_1 itself. For g in G we let $f^g(\rho) = f(\rho^{g^{-1}})$. This gives a consistent group action. Among the subspaces of F_1 , we now single out a special sort.

Definition: A subspace M of F_1 is G - invariant if $M^g = \{f^g : f \in M\} = M$ for all $g \in G$. Such a subspace is called a G - module.

We have the following standard examples: F_1 itself; C , the subspace of constant functions, and $C^{\perp}$, the subspace of functions with integral over Ω equal to zero. To produce other G - modules is a major problem of this method. We will give a construction in the next section.

We can relate the substructures of F_1 to those of G in various ways. One is to start with subsets Δ of Ω and A of F_1 and to set $F_\Delta(A) = \{g \in G \mid \forall f \in A , \forall \delta \in \Delta , f(\delta) = f(\delta^g)\}$. We note that if $A_1 \subseteq A_2$ then $F_\Delta(A_2) \subseteq F_\Delta(A_1)$. Thus if $C \subseteq A \subseteq F_1$ we have $F_\delta(F_1) \subseteq F_\delta(A) \subseteq F_\delta(C)$ where we have taken $\Delta = \{\delta\}$. But $F_\delta(F_1) = G_\delta$ and $F_\delta(C) = G$ so $G_\delta \subseteq F_\delta(A) \subseteq G$.

In general $F_\Delta(A)$ need not be a group, but it is in some special instances.

Lemma 3.4: Suppose that G is transitive on Ω.

(i) If A is G - invariant or Δ is G - invariant then $F_\Delta(A)$ is a subgroup of G.

(ii) $F_\delta(A) = G \Rightarrow A \leq C$, the constant functions.

(iii) $F_\delta(A) = G_\delta \Rightarrow A$ separates points from δ; i.e. $\forall\, \alpha \neq \delta$ $\exists\, f \in A$ such that $f(\alpha) \neq f(\delta)$.

Proof: (i) This is clear if Δ is G - invariant. Suppose A is G - invariant and $g,h \in F_\Delta(A)$. Then $\forall\, \delta \in \Delta$, $f \in A$, $f(\delta) = f(\delta^h) = f^{h^{-1}}(\delta)$. But $f^{h^{-1}} \in A$ so $f^{h^{-1}}(\delta) = f^{h^{-1}}(\delta^g) = f(\delta^{gh})$. Therefore $gh \in F_\Delta(A)$. Moreover, $f(\delta^{g^{-1}}) = f^{g}(\delta) = f^g(\delta^g) = f(\delta)$, so $g^{-1} \in F_\Delta(A)$.

(ii) $F_\delta(A) = G$ implies that $\forall\, g \in G$, $\forall\, f \in A$, $f(\delta) = f(\delta^g)$. But G is transitive so this says that f is constant.

(iii) $F_\delta(A) = G_\alpha$ implies that if $\delta^g \neq \delta$ then $\exists\, f \in A$ such that $f(\delta^g) \neq f(\delta)$. But again since G is transitive this says that A separates points of Ω from δ. □

The first part of the following theorem is a finite version of the Stone-Wierstrass theorem of analysis.

Theorem 3.5: (i) If A is a sub-algebra of F_1 (i.e. if A is closed under multiplication) which contains the constants and separates

points then $A = F_1$.

(ii) If there is a G - invariant sub-algebra A properly contained between C and F_1 then there is a group properly contained between G_α and G and G is imprimitive.

Proof: (i) Let $\alpha \neq \beta$ be points of Ω . Then there is $f \in A$ with $f(\alpha) \neq f(\beta)$. Since A is an algebra containing the constants it contains $f_{\alpha\beta}$ where $f_{\alpha\beta}(\gamma) = f(\gamma)-f(\beta) \;/\; f(\alpha)-f(\beta)$. Now $f_{\alpha\beta}(\alpha) = 1$, $f_{\alpha\beta}(\beta) = 0$ so $\chi_{\{\alpha\}} = \prod_{\beta\neq\alpha} f_{\alpha\beta}$ is in A . Since the characteristic functions are a basis for F_1 , $A = F_1$.

(ii) By the above lemmas $F_\delta(A)$ is a subgroup and clearly $G_\delta \leq F_\delta(A) \leq G$. However, if $F_\delta(A) = G_\delta$ then by the lemma and proof of (i), A contains the characteristic function of δ . But then A is G - invariant and G is transitive (otherwise it is imprimitive), so A contains all characteristic functions and $A = F_1$, a contradiction. Therefore $G_\delta \leq F_\delta(A) \leq G$ and by lemma 1.2, G is imprimitive. □

We can use this theorem to provide a criterion for the triviality of a G - module.

Lemma 3.6: A submodule is invariant by the translations if and only if it is closed under partial differentiation. Hence every G - module is closed under partial differentiation.

Proof: This is Wielandt [12] theorem 18.2, page 82. □

Theorem 3.7: If G is primitive and there is a G - module, M, with a linear differential operator ∂ such that $\partial M = 0$, then $M = \{0\}$ or C.

Proof: Suppose $M \neq \{0\}$. Then since M is closed under partial differentiation it contains the constants. By a linear transformation of the variables we may assume that $\partial \equiv \frac{\partial}{\partial x_1}$. Then the kernel of ∂ is A, the polynomials in F_1 which are independent of X_1. A is clearly an algebra. Now if $\partial M = 0$ and $M > C$, the algebra generated by M satisfies the conditions of theorem (ii) and G is imprimitive. Therefore $M = C$.

3.3 $F_1\, G_\theta$.

There is another subspace of F_1 which is important in the generation of G - modules and the study of G.

Definition: The subspace of G_θ - invariant functions, $\{f : f^g = f \ \forall\, g \in G_\theta\}$ is denoted by $F_1\, G_\theta$.

Lemma 3.8: $\dim_K F_1\, G_\theta$ = rank G = the number of orbits of G_θ.

Proof: Clearly $F_1\, G_\theta$ consists exactly of the functions which are constant on G_θ - orbits. Therefore $\{\chi_\Delta : \Delta$ is an orbit of $G_\theta\}$ is a basis of $F_1\, G_\theta$. □

The isomorphism $\phi : F_1 \to KT$ carries $F_1\, G_\theta$ to a sub-group S of KT, called the Schur ring of G. The following theorem is the key to relating the group theoretic structure of G to the permutation

action of G .

Theorem 3.9: $F_1\, G_\theta$ is closed under convolution.

Proof: As noted earlier convolutions in F_1 are carried over to multiplications in KT . So this assertion is equivalent to the closure of S under multiplication, i.e. to the fact that the Schur ring is indeed a ring. This final result is non-trivial and is proved in Wielandt [11, page 61] for example. □

The importance of $F_1\, G_\theta$ in the construction of G - modules is due to the following theorem.

Theorem 3.10: If $f \in F_1\, G_\theta$ then $f * C^\perp = \{f * h : h \in C^\perp\}$ is a G - module. $f * C^\perp$ is generated by all of the proper partial derivatives of f and moreover $\deg(f*C^\perp) = (\deg f) - 1$.

Proof: See Wielandt [12; page 87]. □

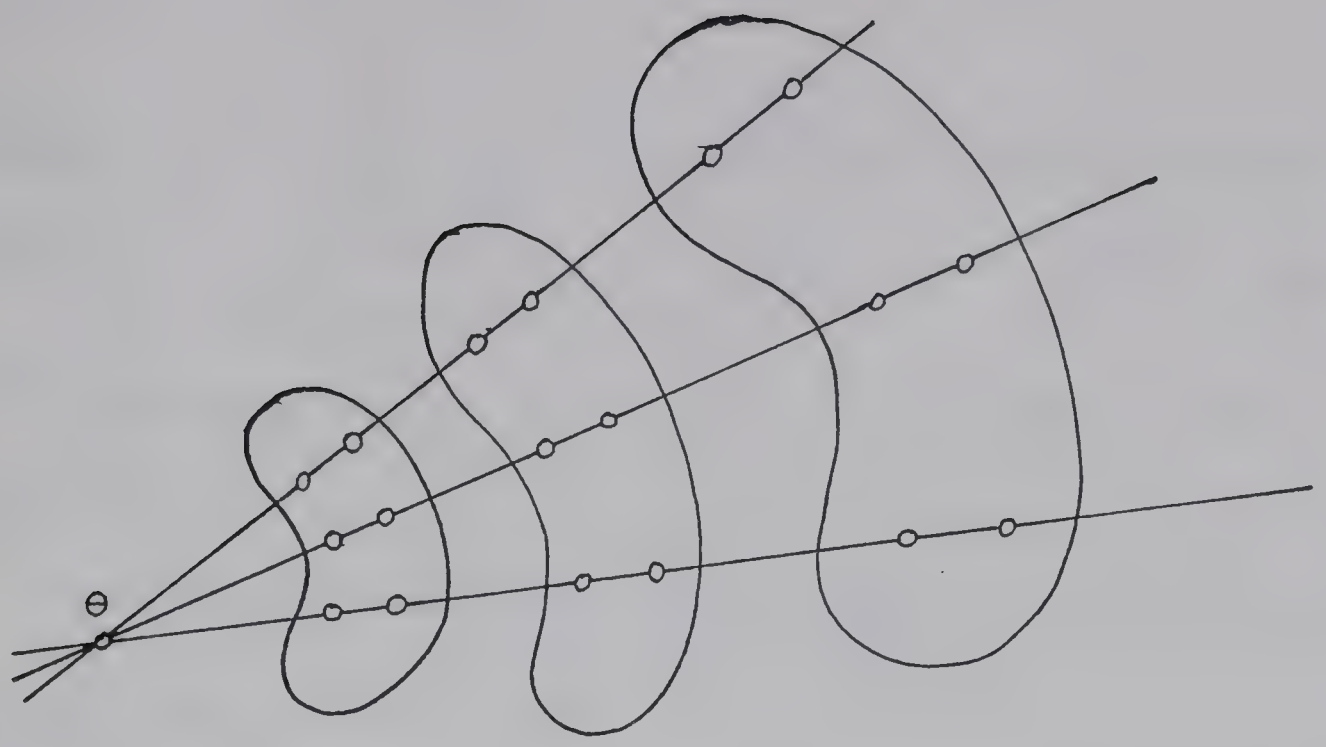
We again identify Ω with $V(n,p)$ and let $\theta = (0,0,\ldots,0)$. This vector space admits mappings of the form $s_m : \delta \to m\delta = (m\delta_1, m\delta_i, \ldots, m\delta_n)$ for $\delta = (\delta_1,\ldots,\delta_n) \in \Omega$, with $m \in \mathbb{F}_p \setminus \{0\}$. These are the dilations and form a group, D . For a subset Δ of Ω let $\Delta^{s_m} = \{\delta^{s_m} : \delta \in \Delta\}$. Then since the elements of D fix θ and "slide" the points of Ω along the lines through θ , Δ and Δ^{s_m} are on the same lines through θ . Furthermore, if ψ_Δ is the set of points on lines through θ and points of Δ , then $\psi_\Delta = \Delta \cup \Delta^{s_2} \cup \ldots \cup \Delta^{s_{p-1}}$.

We want to show that if Δ is a G_θ - orbit then so is Δ^{s_m} for each m. It is enough to do this when $m = r$ is a prime. Take $K = \mathbb{F}_r$. Note that $r < p$. As we have observed S is closed under multiplication in KT and $\phi(\chi_\Delta) = \sum_{t\in\Delta} t$. But we are in characteristic r so $\sum_{t\in\Delta} t^r = (\sum_{t\in\Delta} t)^r$ since the order of the t's is $> r$. However $\phi(\chi_{\Delta^{s_r}}) = \sum_{t\in\Delta} t^r$, so $\chi_{\Delta^{s_r}} \in F_1 G_\theta$. Since $\{\chi_\Delta : \Delta$ is a G_θ - orbit$\}$ is a basis for $F_1 G_\theta$, and the supports of the $\chi_{\Delta^{s_r}}$ for various Δ's are disjoint and since there are as many Δ^{s_r}'s as Δ's, we must have Δ^{s_r} among the orbits of G_θ.

Theorem 3.11: If Δ is an orbit of G_θ and $m \in \mathbb{F}_p \setminus \{0\}$ then Δ^{s_m} is an orbit of G_θ.

As observed before, the set ψ_Δ of lines through θ, touched by Δ is covered by the images of Δ under D. Suppose there is some line λ of ψ_Δ with $|\lambda\cap\Delta| = k$. Then $\forall m$, $|\lambda \cap \Delta^{s_m}| = k$. Moreover there are $\frac{p-1}{k}$ distinct images $\Delta, \Delta^{s_{m_1}}, \ldots, \Delta^{s_{m_{(p-1)/k}}}$ and these partition $\lambda \setminus \{\theta\}$. But these sets must partition every other line of ψ_Δ through θ and the number k is therefore independent of the line λ in ψ_Δ. Also $k|p-1$.

The 2-closure of a transitive group H of permutations on a set Γ, is the largest subgroup of S^Γ which has the same orbits for a point stabilizer as the given group, H. We denote the 2-closure of



H by $H^{(2)}$. We have just shown that $\forall\, s_m \in D$, G_θ and $G_\theta^{s_m}$ have the same orbits. Therefore, G and G^{s_m} have the same 2-closure, call it $G^{(2)}$. Wielandt shows that $G \leq G^{(2)}$ and G is uni-primitive if and only if $G^{(2)}$ is uni-primitive. (Wielandt [12, pg. 10]). The 2-closure has the advantage of being normalized by the dilations. We aim to show that any uni-primitive group containing the translations is in the affine group, so replacing it by a larger uni-primitive group does no harm. Thus we make the following assumption.

Assumption on G : G is a group permuting $\Omega = V(n,p) = AG(n,p)$, $G = G^{(2)}$, i.e. is 2-closed, and G contains T , the translations on Ω .

We note that since each s_m fixes θ , $G_\theta = G_\theta^{s_m}$ also.

The assumption that D normalizes G gives us much more information about F_1 G_θ and G - modules.

Definition: If $f = \sum a_{e_1 \ldots e_n} X_1^{e_1} \ldots X_n^{e_n}$ is in reduced form then set $f^{(n)} = \sum_{e_1+\ldots+e_n \equiv n (\mathrm{mod}\ p-1)} a_{e_1 \ldots e_n} X^{e_1} \ldots X^{e_n}$. $f^{(n)}$ is called the n^{th} homogeneous part of f. If $f = f^{(n)}$ for some n then f is homogeneous.

We now have the following theorem (Wielandt [12, pages 84-85])

Theorem 3.12: Take $f \in F_1$. Then,

(i) $f = f^{(1)} + \ldots + f^{(p-1)}$

(ii) $f^{(n)}(a\rho) = a^n f^{(n)}(\rho)$

(iii) $f \in F_1 G_\theta$ implies $f^{s_m} \in F_1 G_\theta$

(iv) $f^{(n)}(\rho) = - \sum_{\substack{a \in \mathbb{F}_p \\ a \neq 0}} a^{-n} f(a\rho) = - \sum_{s_m \in D} m^{-n} f^{s_m^{-1}}(\rho)$

(v) $f \in F_1 G_\theta$ implies $f^{(n)} \in F_1 G_\theta$ for $n = 1, \ldots, p-1$

(vi) If M is a G - module generated by homogeneous polynomials then $f \in M$ implies $f^{(n)} \in M$ for $n = 1, \ldots, p-1$. □

$F_1 G_\theta$ contains an important subalgebra, denoted $F_1 G_\theta^o$, consisting of the G_θ - invariant functions which are also invariant under the dilations. This is the rational sub-algebra of $F_1 G_\theta$. $F_1 G_\theta^o$ contains exactly the functions that are constant on the sets $\psi_\Delta \setminus \{\theta\}$ with Δ a G_θ- orbit. Since $F_1 G_\theta^o = F_1 (G \rtimes D)_\theta$, where $G \rtimes D$ is the split extension of G by D, $F_1 G_\theta$ is closed under convolution by theorem 3.9. $F_1 G_\theta^o$ is called trivial if it consists of functions constant on $\Omega \setminus \{\theta\}$. This is the case exactly when every orbit of

G_θ , which is not $\{\theta\}$, touches all lines through θ . Uni-primitive groups of degree p^3 with $F_1\, G_\theta^o$ trivial occur for all $p > 2$, (see section 5.1).

By considering the two cases, $F_1\, G_\theta^o$ trivial or not, we can obtain yet more information about $F_1\, G_\theta$. Take the case of $F_1\, G_\theta^o$ trivial first. Suppose h is a homogeneous polynomial in $F_1\, G_\theta$ and that h has a zero not at θ . Then since h is homogeneous, the set of points where h is zero is a union , ψ, of lines through θ . If $h \neq 0$ then $\chi_\psi \in F_1\, G_\theta^o$ and is not constant on $\Omega-\theta$, a contradiction. Therefore any non-zero homogeneous polynomial in $F_1\, G_\theta$ is zero only at θ .

Now if h_1 , h_2 are any two polynomials of the same homogeneous degree, $h_i = h_i^{(n)}$, then for any point ρ of $\Omega-\theta$, $h_o = h_1(\rho)\cdot h_2 - h_2(\rho)\cdot h_1$ is homogeneous and $h_o(\rho) = 0$. Thus h_o is identically zero and h_1 is a scalar multiple of h_2 . By theorem 3.12 (i) and (v), we always have $F_1\, G_\theta = H_1 \oplus \ldots \oplus H_{p-1}$ where H_i consists of the homogeneous functions $h = h^{(i)}$. We have just shown that if $i \neq p-1$, then H_i is at most one dimensional and if $i = p-1$ then H_{p-1} is 2-dimensional, $H_{p-1} = \langle 1, \chi_{\Omega-\theta} \rangle$ (note: we pick up the extra dimension since $1 = \chi_\Omega$ is not strictly a homogeneous polynomial). We have also shown that there is no function in $F_1\, G_\theta$ of degree $s(p-1)$ where $1 \leq s \leq n-1$, since $H_{p-1} = \langle 1, X^{p-1}Y^{p-1}Z^{p-1} \rangle$.

We can say more about the structure of $F_1\, G_\theta$.

Theorem 3.13: If $F_1\, G_\theta^o$ is trivial then there is a homogeneous polynomial $f \in F_1\, G_\theta$ and an integer t , $0 < t \leq p-1$, such that

$$F_1 G_\theta = \langle 1 \rangle \oplus \langle f \rangle \oplus \ldots \oplus \langle f^i \rangle \oplus \ldots \oplus \langle f^t = \chi_{\Omega-\theta} \rangle$$

where Rank G = # of orbits of G_θ on Ω = t+1 .

Proof: The subscripts i with $H_i \neq 0$ form a multiplicative subgroup of $\mathbb{F}_p^*$. Indeed, $f = f^{(n)}$, $g = g^{(m)}$ implies $fg = (fg)^{(mn)}$. But $\mathbb{F}_p^*$ is cyclic so this subgroup has a generator j for some $H_j \neq 0$. Take $f \in H_j$. Then $\forall$ m $f^m \in H_{jm}$ and as m increases we move through all non-zero H's .

The remark on the rank follows from lemma 3.8. □

Note: f may not be of minimal non-zero degree in $F_1 G_\theta$.

Now suppose $F_1 G_\theta^o$ is non-trivial and n = 3 . Recall that ψ_Δ denotes the lines through θ and points of $\Delta \subseteq \Omega$. The non-triviality of $F_1 G_\theta^o$ assures us that there is more than one set ψ_Δ when Δ is restricted to be a G_θ - orbit. Suppose there are t lines through θ in ψ_Δ . Then $f_\Delta = \chi_{\psi_\Delta} + (t-1)\chi_\theta = \sum_{\lambda \subset \psi_\Delta} \chi_\lambda \in F_1 G_\theta$ is a non-constant sum of characteristic functions of lines. Now if π_1 , π_2 Iλ are planes then $\chi_\lambda = (1-\pi_1^{p-1})(1-\pi_2^{p-1}) = 1 - \pi_1^{p-1} - \pi_2^{p-1} + \pi_1^{p-1}\pi_2^{p-1}$. Thus deg f_Δ = p-1 or 2(p-1) .

Consider f*f , and suppose deg f = 2(p-1) . By theorem 3.3, deg $f_\Delta * f_\Delta \leq$ p-1 . But if λ_1 , λ_2 are distinct lines through θ , then by considering the definition of convolution we see that $\chi_{\lambda_1} * \chi_{\lambda_2} = \chi_\pi$ where π is the plane (through θ) generated by λ_1 and λ_2 . Also $\chi_{\lambda_1} * \chi_{\lambda_1} = 0$. Therefore $f_\Delta * f_\Delta$ is a sum of

characteristic functions of planes. Thus deg $f_\Delta * f_\Delta = 0$ or $(p-1)$.

Therefore we either have a function in $F_1 G_\theta$ of degree $p-1$ or else $f_\Delta * f_\Delta$ is a constant for every Δ. Actually we must have $f_{\Delta_1} * f_{\Delta_2} \in C$ for any two G_θ orbits Δ_1 and Δ_2 by an identical argument. It seems very unlikely that all of these convolutions should end up in C. We can as yet only offer the following however:

Theorem 3.14: If $F_1 G_\theta$ is non-trivial and $p = 3$ then $F_1 G_\theta$ contains a function of degree 2 $(n=3)$.

Proof: We have only to show that there is no possible collection of sets of lines ψ_{Δ_i} with $f_{\Delta_1} * f_{\Delta_2} \in C$ for every pair of orbits, Δ_1, Δ_2.

By theorem 3.15 (below) no orbit of G_θ is contained in a subspace so there must be at least 3 lines in each ψ_Δ and the lines are not in a plane. Since we can replace ψ_Δ with the lines through θ it doesn't contain we may therefore assume that ψ_Δ consists of 3, 4, 5 or 6 of the thirteen lines through θ in $AG(3,3)$.

In the first place $f_\Delta * f_\Delta \in F_1 G_\theta^o$ for any choice of K so must be constant at least on ψ_Δ for any K. If we represent the lines of ψ_Δ by points on π_∞ then by a straight forward case study we have the following possibilities which satisfy this initial criterion for $K = \mathbb{F}_p$ (Figure 0). (iii) is not possible, since with $K = Q$, the rational numbers, we end up with a G_θ - orbit contained in a line, contrary to 3.15. None of the other configurations give a ψ_Δ with $f_\Delta * f_\Delta$ constant. Therefore deg $(f*f) = p-1 = 2$.

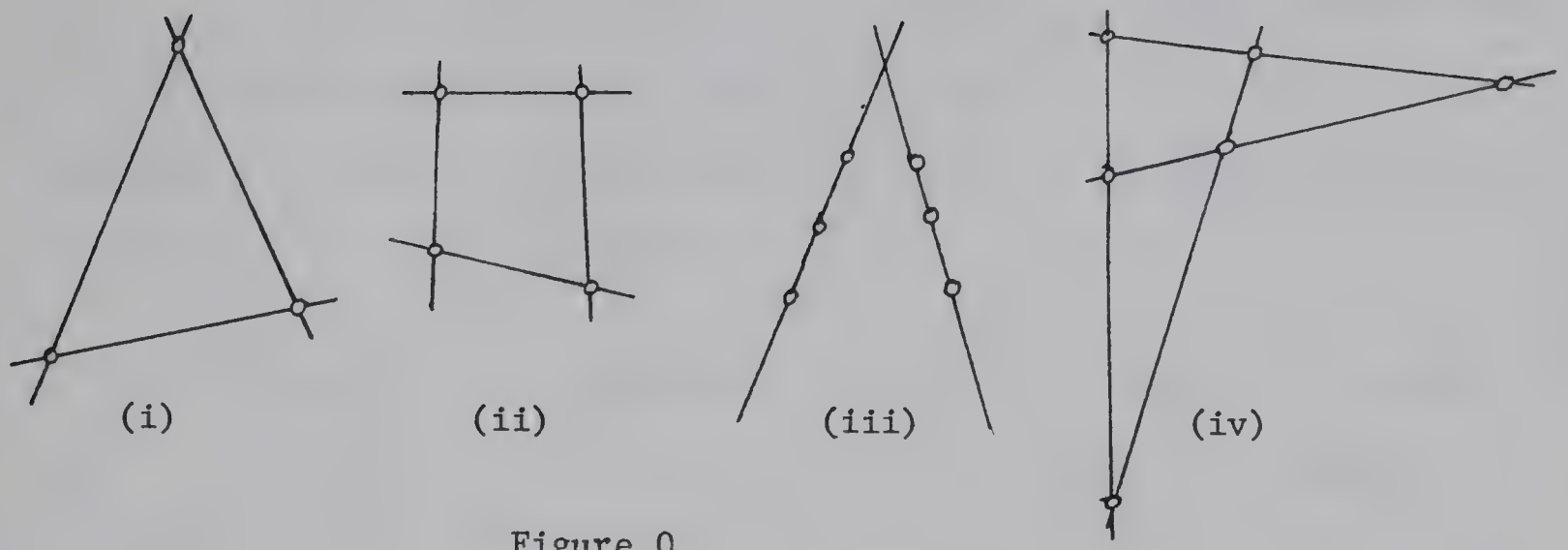


Figure 0

We conclude this section on $F_1\, G_\theta$ with an important characterization of primitivity in G .

Theorem 3.15: G is primitive if and only if no orbit of G_θ lies in a proper subspace of $\Omega = V(n,p)$.

Proof: ($\rightarrow$) Throughout this proof only we take $K = \mathbb{Q}$. Suppose Δ is a G_θ - orbit which generates a proper subspace, Γ , of Ω . Then $\chi_{\psi_\Delta} \in F_1\, G_\theta$. We look at $f = \chi_{\psi_\Delta} * \chi_{\psi_\Delta}$. By definition,

$f(\rho) = \int_\Omega \chi_{\psi_\Delta}(\rho-\omega)\chi_{\psi_\Delta}(\omega) = \int_{\rho=\omega_1+\omega_2} \chi_{\psi_\Delta}(\omega_1)\cdot\chi_{\psi_\Delta}(\omega_2)$. Thus $f(\rho) > 0$ if and only if ρ is in the subspace spanned by θ and two points of ψ_Δ (i.e. the ω_1 , ω_2 with $\rho = \omega_1+\omega_2$). As we continue we find that $(\chi_{\psi_\Delta})^{*i}$, the i^{th} convolution power of χ_{ψ_Δ} , is positive exactly on the points ρ of Ω with $\rho = \omega_1 + \ldots + \omega_i$ for some ω_j's in ψ_Δ . Thus for sufficiently large i , $(\chi_{\psi_\Delta})^{*i}$ is positive exactly on Γ . Therefore $\chi_\Gamma \in F_1\, G_\theta$.

Now take $(\alpha_1,\ldots,\alpha_n) \in \Gamma\backslash\theta$. Then $\partial \equiv \sum_i \alpha_i \frac{\partial}{\partial x_i}$ annihilates χ_Γ and all derivates of χ_Γ . But $M = \chi_\Gamma * C^\perp$ is a non-constant G - module and is generated by the derivates of χ_Γ . Therefore $\partial(M) = 0$. By theorem 3.7, G is imprimitive.

($\leftarrow$) Suppose G is imprimitive and Γ is a block of G containing θ . By the proof of theorem 4.2 (which is proved independently of any other results in this thesis), Γ is a proper subspace of Ω . Thus if $P \in \Gamma\backslash\theta$ then the G_θ - orbit, $\Delta = P^{G_\theta}$, is necessarily in Γ . $\square$

CHAPTER IV

The Problem

4.1 We restrict ourselves now to the case with $n = 3$. The following theorem provides an initial classification of permutation groups of degree p^3.

Theorem 4.1: If $\Omega = AG(3,p)$, G permutes Ω and G contains T, the translations on Ω, then one of the following is true:

(i) $T \lhd G \leq Aff(3,p)$.

(ii) G (a) is imprimitive or (b) contains an imprimitive subgroup of index 3 which is normal or contains an index 2 subgroup which is normal in G.

(iii) There are no planes π such that π^g is a plane for every $g \in G$ and either

(a) there is no line λ such that λ^g is a line for all $g \in G$, or

(b) there is an orbit Δ of G_θ which contains points of at most $p+1$ lines through θ and no 3 of these lines are coplanar or

(c) $p = 2$.

Proof: We require a technical lemma from Wielandt [12] which is contained in the proof of his theorem 16.4 on page 69.

Lemma: Let g act on $AG(2,p)$ so that $A_i^g = A_i$ $(i=1,2,3)$ for three non-collinear points and such that each of the parallel pencils generated by A_iA_j $(i \neq j)$ consists of lines mapped to lines by g. Then g is

the identity.

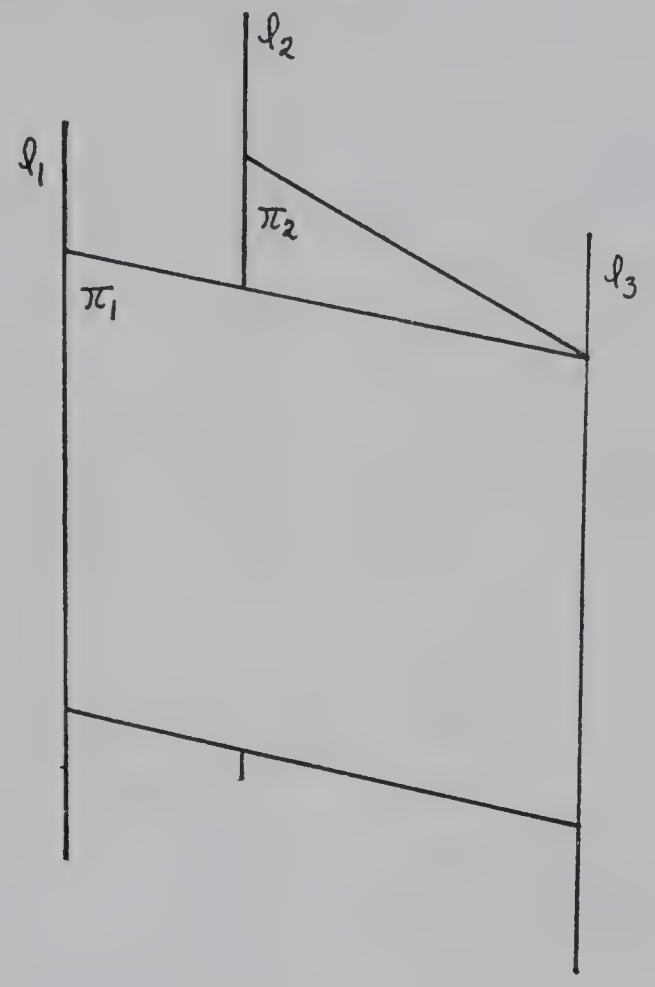
For the proof of the theorem let $\Lambda = \{\lambda \mid \lambda^g$ is a line for all $g \in G\}$ and $\Pi = \{\pi \mid \pi^g$ is a plane for all $g \in G\}$. Since $T \leq G$, Λ and Π are unions of parallel pencils of lines and planes respectively. If we view Ω as embedded in a projective 3 - space then each of the pencils in Λ determines a unique point on π_∞, the plane at infinity, and each of the pencils in Π determines a line on π_∞. Let S be the set of points, L the set of lines, so determined on π_∞ and let $J = \langle S, L\rangle$ be the incidence structure they inherit from π_∞.

If P_1, P_2 are parallel pencils of planes in Π then $P_1 \cap P_2 = \{\pi_1 \cap \pi_2 : \pi_i \in P_i\}$ is a parallel pencil of lines which belong to Λ. Therefore J is closed under the intersection of lines. Note that if $\hat{P} \in L$ is the line coming from $P \subset \Pi$ and $\hat{\}} \in S$ comes from $\} \subset \Lambda$, then $\hat{P}$ I $\hat{\}}$ if and only if every line of $\}$ is incident with some plane of P and vice versa. Let $S^* \subset S$ be those points of S which are incident with at least 2 lines of L. Let $J^* = \langle S^*, L\rangle$.

We assert that G acts as a permutation group of J^*, preserving incidences. Indeed if $\pi_1 \parallel \pi_2$, $\pi_i \in \Pi$ then for any $g \in G$, π_1^g, π_2^g are planes and $\pi_1^g \cap \pi_2^g = (\pi_1 \cap \pi_2)^g = \phi$. Thus G permutes the pencils in π as units, so G permutes the lines L of J^* consistently.

Now if $\hat{\}} \in S^*$ then $\hat{P}_1 \cap \hat{P}_2 = \hat{\}}$ for some pencils P_1, P_2 of planes in π. Take $\ell_1, \ell_2 \in \}$. Then there are planes $\pi_i \in P_i$ such that π_i I ℓ_i. Also $\pi_1 \not\parallel \pi_2$ so $\ell_3 = \pi_1 \cap \pi_2$ is a line and

$\ell_3 \in \rbrack = P_1 \cap P_2$. But then ℓ_1^g , ℓ_3^g are lines in π_1^g ; $\ell_1^g \cap \ell_3^g = (\ell_1 \cap \ell_3)^g = \phi$. Thus ℓ_1^g is parallel to ℓ_3^g . Similarly $\ell_2^g \parallel \ell_3^g$ and finally $\ell_1^g \parallel \ell_2^g$. Thus $\rbrack^g$ is a parallel pencil in Λ and $\hat{\rbrack}^g = \hat{P}_1^g \cap \hat{P}_2^g$ so $\hat{\rbrack}^g \in S^*$. Thus G also permutes the points in S^* . That incidence is preserved is clear.



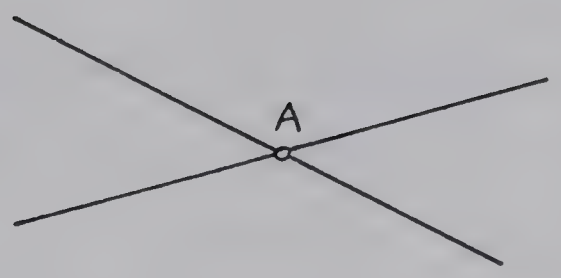
Now if G acting on J^* fixes an element, line or point, then G permutes the elements of this pencil amongst themselves and G is imprimitive.

We examine the possibilities for J^* . J^* is closed under intersection of lines. Therefore it is one of the following types. (See for example Albert and Sandler [1, page 7].)

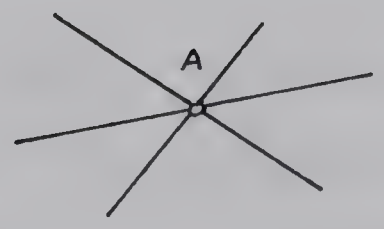
(o) $|L| = 0$

(i) $|L| = 1$, $J^* \equiv$ 

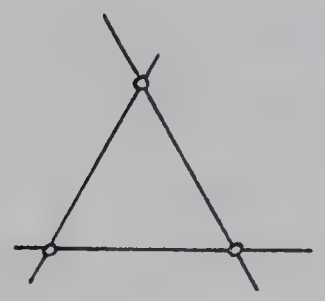
(ii) $|L| = 2$, $J^* \equiv$



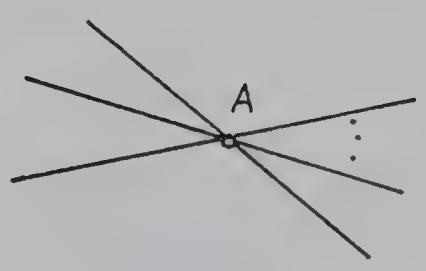
(iii) $|L| = 3$, (a) $J^* \equiv$



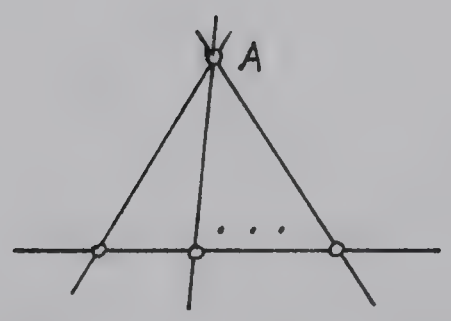
or, (b) $J^* \equiv$



(iv) $|L| \geq 4$, (a) $J^* \equiv$



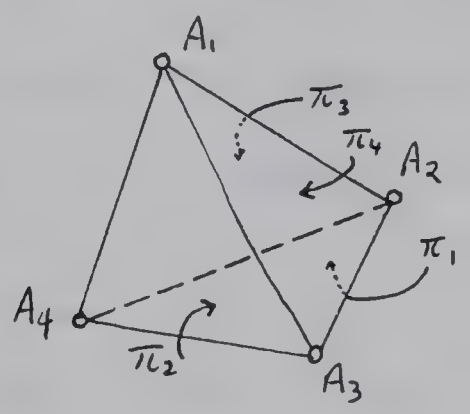
(b) $J^* \equiv$



(c) J^* contains a quadrilateral

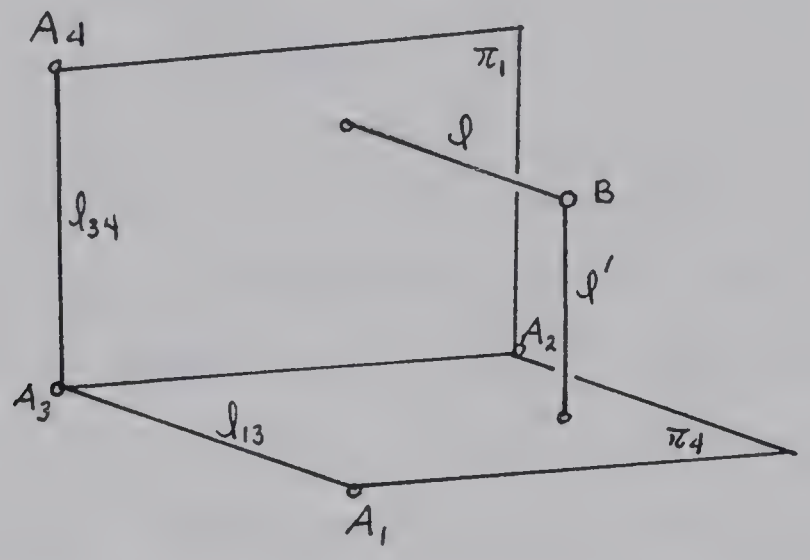
In case (i), the line is fixed and G is imprimitive. In cases (ii), (iii)(a), (iv)(a) and (b) the point A is fixed so G is again imprimitive. In the case (iii)(b) the stabilizer of an edge has index 1 or 3 and is imprimitive. The stabilizer of the triangle has index 1 or 2 in this stabilizer of an edge and is normal in G.

We will show that in case (iv)(c), $G \leq \mathrm{Aff}(3,p)$. Since $T \lhd \mathrm{Aff}(3,p)$, $T \lhd G$ will then follow. The configuration (iv)(c) implies that we can find in Ω, four planes of Π no three of which are co-axial, π_1, π_2, π_3, π_4. Take $g \in G$ and let $A_i = \pi_j \cap \pi_k \cap \pi_l$ for $\{i,j,k,l\} = \{1,2,3,4\}$. Then we can find an $h \in \mathrm{Aff}(3,p)$ such that $A_i^{gh} = A_i$ for $i=1,2,3,4$, since $\mathrm{Aff}(3,p)$ is transitive on the sets of 4 independent points. (This follows since $GL(3,p)$ is transitive on the bases of $V(3,p)$.) Then since gh maps each π_i to a plane it fixes these planes.



We claim that each plane is fixed pointwise by gh. Consider π_1. Let $\ell_{ij} = A_iA_j$. Then every line of π_1 which is parallel to ℓ_{ij} is mapped to a line of π_1, (parallel to $\ell_{ij}^{gh} = \ell_{ij}$) for $1 \neq i \neq j \neq 1$. Thus the lemma of Wielandt applies and $gh\big|_{\pi_1}$ is the identity. Similarly gh fixes π_2, π_3 and π_4 pointwise.

Now if $B \in \Omega$, not on π_i for $i = 1,2,3,4$ then $\exists \ell, \ell'$ I B such that $\ell \parallel \ell_{13}$, $\ell' \parallel \ell_{34}$. Then $\ell^{gh} \parallel \ell$ and $\ell^{gh} \cap \pi_1 = \ell \cap \pi_1$. Therefore $\ell^{gh} = \ell$. Similarly $\ell'^{gh} = \ell'$. Finally $B^{gh} = (\ell \cap \ell')^{gh} = \ell \cap \ell' = B$. Thus gh = identity, $g = h^{-1}$ and $g \in \mathrm{Aff}(3,p)$. Therefore $G \leq \mathrm{Aff}(3,p)$.



If $|L| = 0$ then there are no planes whose image under every $g \in G$ is a plane. $|S^*| = 0$, but we may have $|S| > 0$, i.e. pencils in Λ. In this situation it is conceivable that there are parallel pencils in Λ which are not mapped to single parallel pencils by every element of G.

Claim: If $|L| = 0$ then S can not contain three collinear points if $p > 2$. Indeed if $\hat{\rbrace}_1$, $\hat{\rbrace}_2$, $\hat{\rbrace}_3$ are collinear points of S with $\hat{\rbrace}_i$ coming from the line pencil $\rbrace_i$ then there is a parallel pencil of planes P such that every plane π of P contains lines from each of $\rbrace_1$, $\rbrace_2$, $\rbrace_3$. Choose $\ell_i \in \rbrace_i \cap \pi$ for some $\pi \in P$, non-concurrent. Let $A_i = \ell_j \cap \ell_k$ with $\{i,j,k\} = \{1,2,3\}$. We can find $h \in \mathrm{Aff}(3,p)$ such that gh fixes A_i, $i = 1,2,3$. Then $\ell_i^{gh} = \ell_i$ for $i = 1,2,3$. We will show that $\pi \in \Pi$.

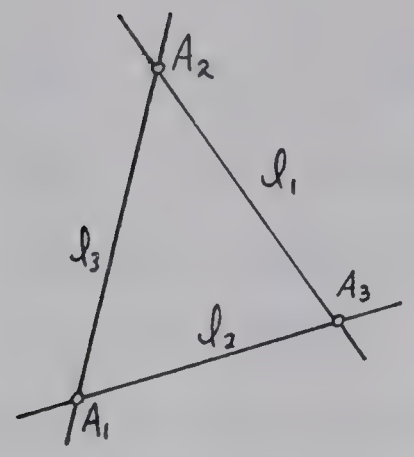


Figure I

Now take any point $B \in \pi$. B is on a line $\ell \parallel \ell_1$ (Figure II). Unless ℓ I A_1 , ℓ contains two points, namely $\ell \cap \ell_2$ and $\ell \cap \ell_3$, which have gh images in π . But ℓ^{gh} is a line, so $\ell^{gh} \subset \pi$. But if $BA_1 \parallel \ell_1$ we can use the line incident with B and parallel to ℓ_2 or ℓ_3 . This will fail only if $\forall i$, $BA_i \parallel \ell_i$. But then we have the configuration of Figure III. This is Aff(3,2) and p = 2 .

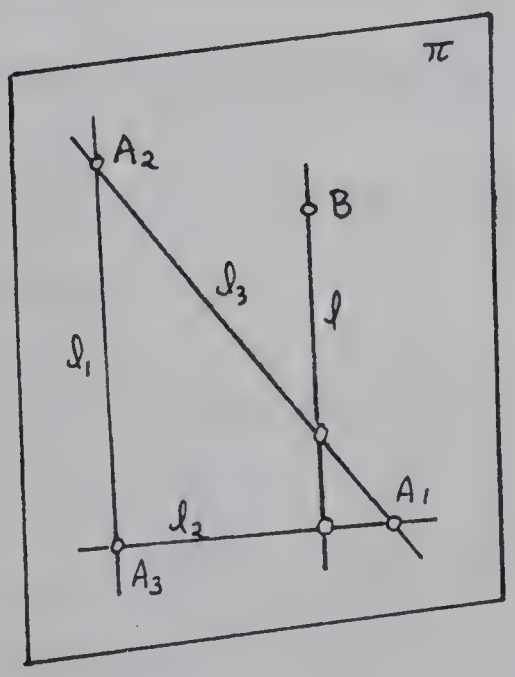


Figure II

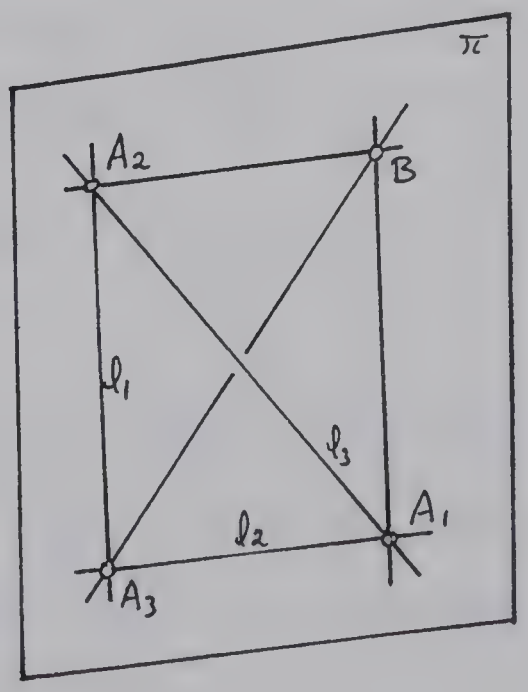


Figure III

So we have shown that if $|L| = 0$ then the points of S form a k - arc where $k = |S|$ in the language of Dembowski [7], i.e. no 3 are collinear. Thus $|S| \leq p+1$ since $p \neq 2$ (Dembowski, page 149). Now if (iii)(a) and (c) do not hold, we have $|S| > 1$ and there are lines through θ which are always mapped to lines by G and hence by G_θ. We have shown that there are at most $p+1$ such lines and no three are coplanar. If we take Δ as any G_θ orbit of points on these lines we are done and case (iii)(b) holds. □

In the corresponding classification of groups of degree p^2, Wielandt showed that groups of type (iii) must by multiply transitive. We have only partial results in this direction, though, in the case of degree p^3. The conjecture is that all primitive groups of the final type (iii) are multiply transitive or are in $Aff(3,p)$.

As an addendum to the above theorem we note that even if $|L| = 0$ and G is imprimitive, the blocks still must be linear.

Theorem 4.2: If G is imprimitive then the blocks of G are either lines or planes.

Proof: Let ψ be a block, $\alpha,\beta \in \psi$. Then since G contains a translation t such that $\alpha^t = \beta$, $\psi^t = \psi$ and the whole line through α and β, i.e. $\alpha^{<t>}$, is in ψ. Thus ψ is a linear subspace, i.e. a line or a plane. □

4.2 Criteria.

It is evident that if we are to elucidate the case (iii) of theorem 4.1, we must find a way of keeping careful scrutiny of the G images of planes and lines.

The next theorem provides a general classification of a certain type of function. This can be used to keep track of planes in Ω. It is proved for a general dimension.

Theorem 4.3: If f maps $AG(n,p)$ to $\{0,\pm 1\}$ in $\mathbb{F}_p, p\neq 2, n\geq 2$, $\int_\lambda f = 0$ for every line λ and f has at most p^{n-1} zeros, then either,

(i) f is constant but not zero, or

(ii) f has exactly p^{n-1} zeros and they form an $(n-1)$ - dimensional linear sub-variety.

Proof: For the sake of brevity we will abbreviate linear subvariety to 1.-s. We decompose the proof into several steps. Assume f satisfies the hypotheses.

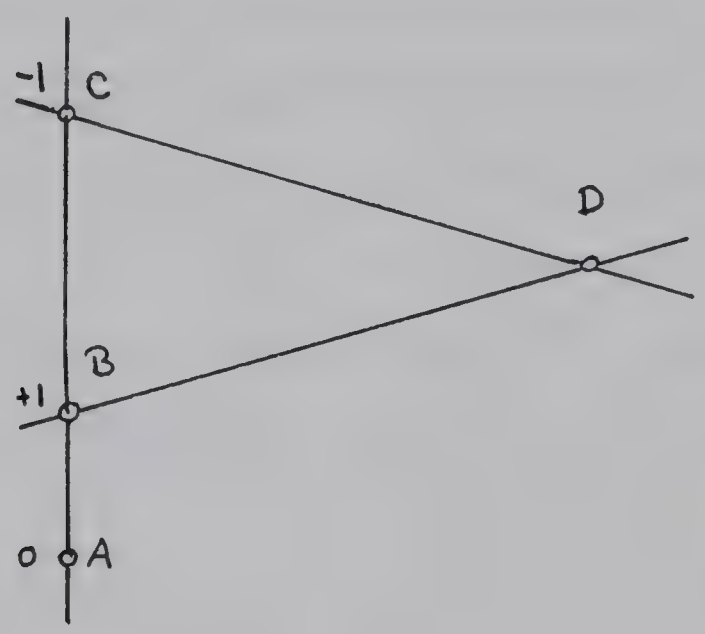
(i) f is constant on any 1.-s. where it has no zeros:

Let λ be a line and suppose f has value $+1$ m times on λ and is never zero on λ. Then since $\int_\lambda f = m-(p-m) = 2m-p \equiv 0 \pmod p$ and $p \neq 2$, $m = 0$ or p and f is constant on λ. Now let γ be a 1.-s. and suppose f has no zeros on γ. Then f is constant on every line of γ and hence is constant on γ.

(ii) Suppose π is a k - dimensional 1.-s. of $AG(n,p)$ with

$k \geq 2$. Then f can not have a unique zero on π .

Let A be the unique zero of f on π . If λ is a line of π , $\lambda \mathrm{I} A$, then since $\int_\lambda f = 0$ there are points, B and C , on λ such that $f(B) = +1$, $f(C) = -1$. Now since $\dim(\pi) \geq 2$ there is a point of π not on λ ; call it D . The lines DB , DC do not contain A so f has no zero on them. Thus f is constant on these lines. But then $+1 = f(B) = f(D) = f(C) = -1$, a contradiction.

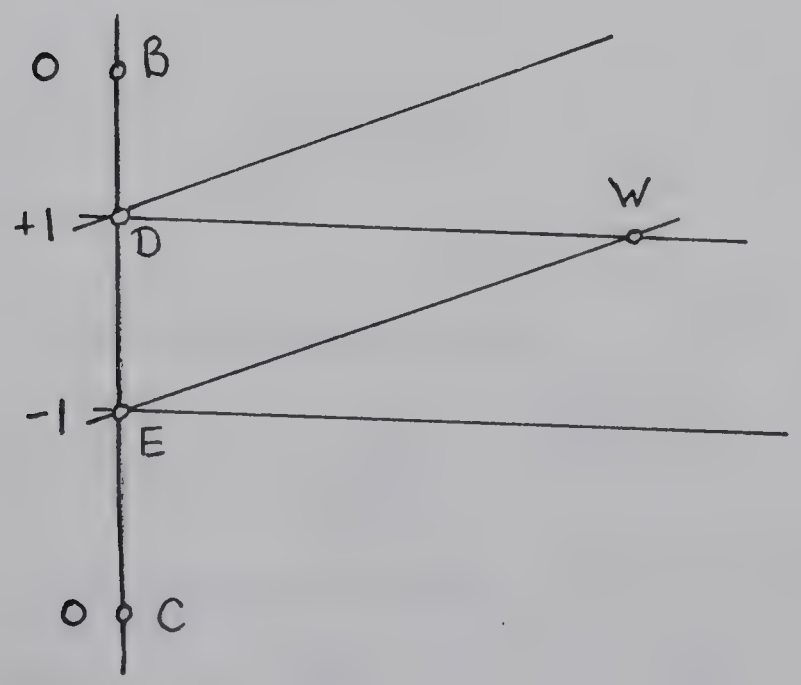


We now prove the theorem by induction on n . We do this by in fact proving that the following assertion holds and that the theorem holds for each succesive n :

(*) If η is a k - dimensional l.-s. of $AG(n,p)$, with $0 \leq k \leq n-2$, such that $f|\eta$ is a non-zero constant then there is a $(k+1)$ - dimensional l.-s., η' , with η contained in η' and $f|\eta'$ a constant.

For $n = 2$, we have the affine plane and f has $\leq p$ zeros. Suppose $f(A) \neq 0$. There are $p+1$ lines of Ω through A and so one of them contains no zero. Then by (i) f is constant on this l.-s.

For the theorem when $n = 2$, we know that f can not have a unique zero and if it is not a constant it must have at least one zero since $\int_\lambda f = 0$ for every line. Thus there is a line joining two points B and C with $f(B) = f(C) = 0$. If $f\big|_{BC}$ is not zero there are points D and E on BC with $f(D) = +1$, $f(E) = -1$. There are p lines through each of these points without counting BC and each of these pencils of lines partitions the zeros of f not on BC . There are at most $p-2$ zeros not on BC so we have at least 2 lines through each of D and E where f is constant. These lines can't all be parallel so we find a point W with $+1 = f(D) = f(W) = f(C) = -1$, a contradiction. Therefore $f\big|_{BC}$ is zero and the theorem is true in dimension 2.



Now suppose that the theorem is true for dimensions less than n . We will show that (*) is valid and from this that the theorem is true for dimension n .

η is contained in $(p^{n-k}-1)/(p-1)$ 1.-s. of dimension $k+1$ (Biggs [6], page 37). Let m of these contain no zeros of f . By (i), f is constant on each of these, so it is enough to show that $m \geq 1$. Each of the $\{\frac{p^{n-k}-1}{p-1} - m\}$ varieties where f is not constant is an $AG(k+1,p)$ and $k+1 < n$ by assumption. Therefore f has $\geq p^k$ zeros on each of these varieties by induction. These varieties intersect in pairs at η so these zeros are distinct. We have counted at least $\{\frac{p^{n-k}-1}{p-1} - m\} \cdot p^k$ zeros and f has at most p^{n-1} zeros. Therefore,

$$p^{n-1} \geq p^k \{\frac{p^{n-k}-1}{p-1} - m\}$$

so

$$m \geq \frac{p^{n-k}-1}{p-1} - p^{n-k-1} = \frac{p^{n-k-1}-1}{p-1} \quad .$$

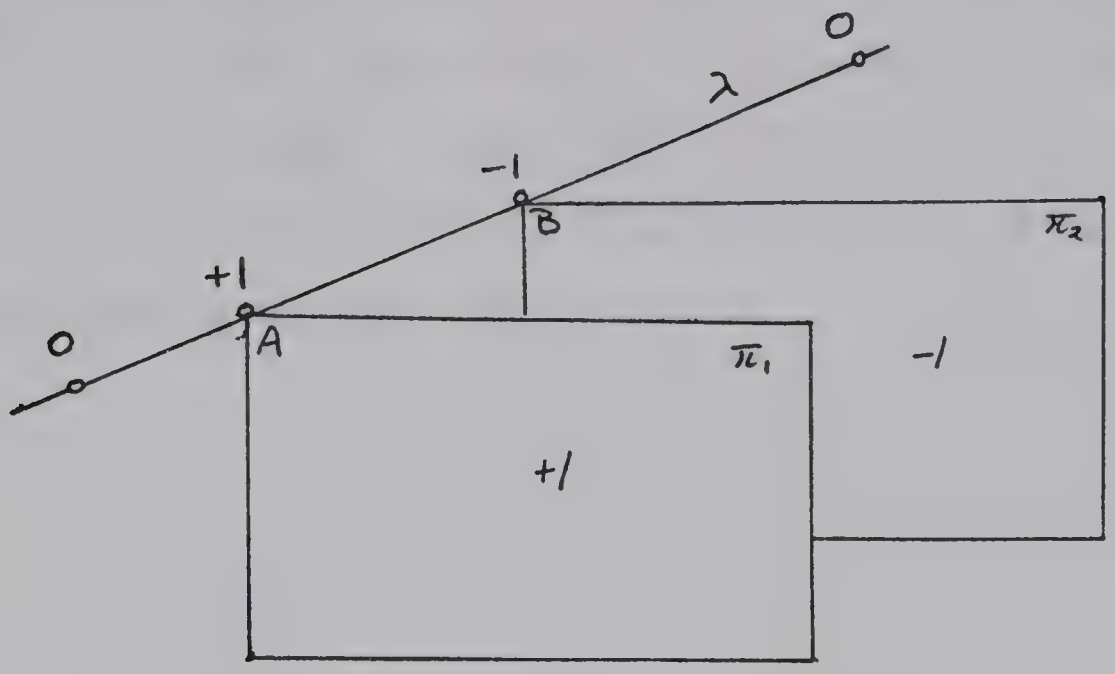
But this says that if $n \geq k+2$ then $m \geq 1$. So (*) is established for all η .

For the theorem in dimension n now we need,

(iv) If a line λ contains 2 zeros of f then $f|_\lambda \equiv 0$.

Indeed, suppose $f|_\lambda \not\equiv 0$. Then since $\int_\lambda f = 0$, there are points A and B on λ with $f(A) = +1$, $f(B) = -1$. Now by (*) used over and over there are hyperplanes π_1 , π_2 such that $f|_{\pi_1} = +1$,

$f|_{\pi_2} = -1$ and $A \text{ I } \pi_1$, $B \text{ I } \pi_2$.

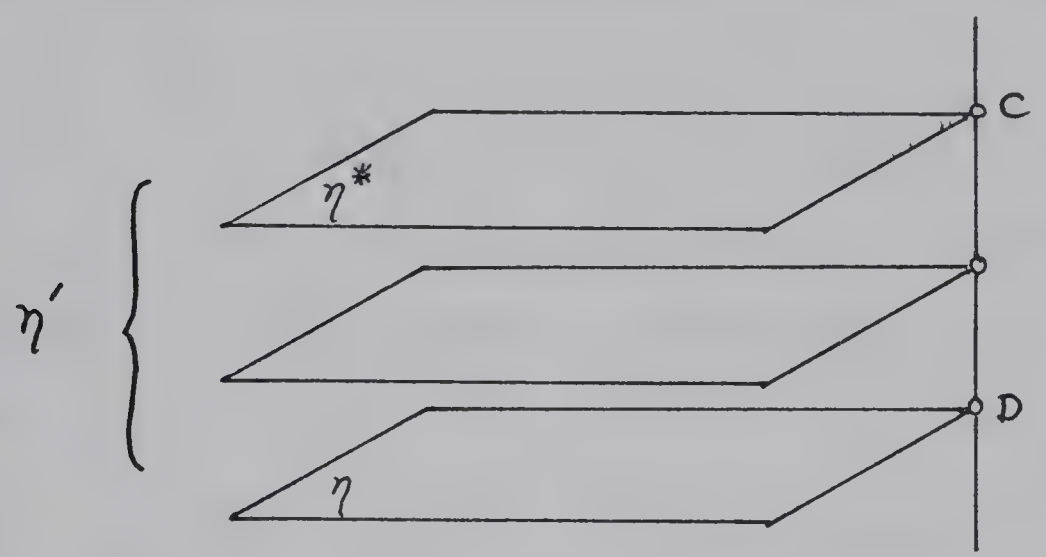


The hyperplanes π_1 , π_2 must be parallel. Thus every line of the pencil parallel to λ intersects each of π_1 and π_2 , i.e. f is not constant on any of these p^{n-1} lines. By (i) f has at least one zero on each of these lines and we know that it has two zeros on λ ; a contradiction, since f has at most p^{n-1} zeros. Hence $f|_\lambda$ is zero.

Now for the theorem in dimension n . If f is not constant then f has a zero, A .

Suppose η is a linear subvariety of dimension $k \leq n-2$ such that $f|_\eta \equiv 0$. Then there is a 2 - dimensional l.-s. π such that $|\eta \cap \pi| = 1$, (since co-dimension $\eta \geq 2$). Now by (ii) since f has one zero on π it has another. Therefore, there is a zero, C , of f outside η . Let η' be the l.-s. spanned by η and C .

Claim: $f|_{\eta'}$ is zero. Let $D \in \eta$; then $f|_{DC}$ is zero by (iv). Therefore f is zero at all points of η' which are on lines joining C to points of η. This includes all of η' except the k - dimensional l.-s. of η', through C and parallel to η; call it η^*. But if $p > 2$ there is a point of η' in neither η nor η^* and we can repeat the argument from this point. Thus $f|_{\eta'}$ is zero.



We can continue this process as long as $\dim(\eta) \leq n-2$. Therefore, there is a hyperplane π such that f is zero on π. Since π has p^{n-1} points and f has at most p^{n-1} zeros the theorem follows. □

The criterion of theorem 4.3 is useful for the following reason. If $\pi = a_1X_1 + \ldots + a_nX_n + b$ with $a_i \in \mathbb{F}_p$ then $\pi = 0$ has exactly p^{n-1} solutions in Ω, the points of the hyperplane π. Now $\pi : \Omega \to \mathbb{F}_p$, so $\pi^{(p-1)/2} : \Omega \to \{0, \pm 1\} \subseteq \mathbb{F}_p$ since the multiplicative group of $\mathbb{F}_p$ is cyclic of order $(p-1)$. Therefore if we can find a function $f = \pi^{(p-1)/2}$ in a G - module M with degree $(M) < p-1$, then we know that the G images of f satisfy the hypotheses of theorem 4.3 and the zeros of f are a hyperplane in Π (where this is the

Π of theorem 4.1).

If we take our field K to be $\mathbb{F}_{p^2}$ then we can also find functions which have small degree and represent lines in some way. We restrict ourselves to $n = 3$.

Theorem 4.4: If the plane $\ell = 0$ of $AG(3,p^2)$ is parallel to a plane of $AG(3,p)$, considered as a subgeometry of $AG(3,p^2)$, then ℓ takes on exactly p values on $AG(3,p)$ and its level surfaces there are planes. If ℓ is not parallel to a plane of $AG(3,p)$, then ℓ takes all p^2 values in $\mathbb{F}_{p^2}$ on $AG(3,p)$ and its level surfaces are lines. In particular, in the latter case, ℓ has exactly p zeros and they are a line.

Proof: $\ell = a_1X_1 + \ldots + a_3X_3 + a_o$. ℓ is parallel to a plane of $AG(3,p)$ if and only if there is some $\lambda \in \mathbb{F}_{p^2} \setminus \{0\}$ such that $\forall_{i\neq 0}$, $\lambda a_i \in \mathbb{F}_p$. Suppose ℓ is parallel to a plane of $AG(3,p)$. Then $\lambda(\ell-\alpha_o)$ is a plane of $AG(3,p)$ for some $\alpha_o \in \mathbb{F}_{p^2}$ so takes on each value in $\mathbb{F}_p$ exactly on a plane (parallel to ℓ). Therefore ℓ takes on every value in $\lambda^{-1}\mathbb{F}_p + \alpha_o$ and the level surfaces are the same as for $\lambda^{-1}\ell - \alpha_o$.

Now suppose that ℓ is not parallel to a plane of $AG(3,p)$. This means that $\forall\alpha_o \in \mathbb{F}_{p^2}$, $\ell - \alpha_o$ has at most a collinear set of zeros on $AG(3,p)$. Thus ℓ takes the value α_o on at most p points for each α_o in $\mathbb{F}_{p^2}$. But there are only p^3 points in $AG(3,p)$, so ℓ takes each value p times and the level surfaces are lines. □

4.3. L and p = 3 .

Restricting ourselves to $n = 3$, we denote the variables by X , Y and Z . We study now the G - module generated by the linear functions over K , i.e. $L = \langle X,Y,Z\rangle^G$. The functions in L measure in some way the extent to which a linear function is changed by G , so L measures how much the planes and if $K = \mathbb{F}_{p^2}$, by theorem 4.4, the lines are distorted by G .

Theorem 4.5: Let ℓ be a linear function over K and $L' = \langle \ell \rangle^G$. If $\deg L' \leq p-1$ then $L' = L$.

Proof: Let H be the subspace of L' consisting of the linear forms in L' , where by a form we shall mean a function with terms of only one degree. Then since $\ell \in L'$, $\dim_K H \geq 1$. Suppose $L \neq L'$. Then L' does not contain all of X , Y and Z so $\dim_K H = 1$ or 2 . Therefore by a linear change of variables we can consider H as a subspace of $\langle X,Y\rangle = \ker \frac{\partial}{\partial Z}$. Hence, there is some differential operator, ∂ , such that $\partial H = 0$.

Take $f \in L'$. We will show that $\partial f = 0$. Since $f = f^{(0)} + f^{(1)} + \ldots + f^{(p-1)}$ it is enough to consider f homogeneous. And since $\deg f = t \leq p-1$, f is in fact a form. Now suppose $\partial f = h \neq 0$. Then h is a form so there is a differential operator D such that $Dh = c \neq 0$, c a constant. But since Dh is a non-zero constant, D has order $t-1$. Thus Df is linear or zero, and so certainly ∂Df is zero. But $\partial Df = D\partial f = Dh = c \neq 0$, a contradiction. Therefore $\partial(L') = 0$. But now we have a G - module properly containing the constants and annihilated by a linear differential operator. By

theorem 3.7, this is impossible. Hence $L' = L$. □

This theorem shows that if M is a G - module with $M > C$, $\deg M \leq p-1$, then $L \leq M$. For, M being a G - module is closed under differentiation and hence contains a linear function. But then $\langle \ell \rangle^G \leq M$ so $\deg \langle \ell \rangle^G \leq p-1$ and $L \leq M$.

Let m denote the smallest degree of a non-constant function in $F_1 G_\theta$ and suppose, $f \in F_1 G_\theta$, $\deg f = m$. Then if $m \leq p$, $M = f * C^\perp$ has degree $\leq p-1$ and $\deg L \leq p-1$. Moreover if $m \leq p-1$ then $1 \leq \deg L \leq p-2 - \deg f * C^\perp$. Take $p = 3$. This reduces to $\deg L = 1$.

Now by theorem 3.14, there is such a function f when $p = 3$ and $F_1 G_\theta^o$ is non-trivial, so $\deg L = 1$ in this case. But now we know that linears are mapped to linears by G , so planes are preserved and $G \leq \mathrm{Aff}(3,3)$.

Theorem 4.6: If G is primitive of degree 27, $G \geq T$, an elementary abelian regular subgroup ,then either

(i) $T \lhd G \leq \mathrm{Aff}(3,3)$, or

(ii) G is 2 - transitive.

Proof: We have only to deal with the case where $F_1 G_\theta^o$ is trivial. Let Δ be an orbit of G_θ , $\Delta \neq \{\theta\}$. Then Δ contains k points from each line through θ and $k \mid p-1$. Here $p = 3$ so $k = 1$ or 2 .

If $k = 2$, then $\Delta = \Omega - \theta$ and G is 2 - transitive. If $k = 1$ then G_θ has exactly one other non-trivial orbit, namely $-\Delta$.

Thus G_θ is rank 3 with stabilizer orbits of length 1, 13 and 13. The lemmas 5 and 7 of D.G. Higman [9, page 148-50] show that we can not have $o(G)$ even. If $o(G)$ is odd then the Feit-Thompson theorem assures us that G is solvable. A primitive solvable group always contains a regular normal elementary abelian subgroup. Thus theorem 2.1 shows that $G \leq \mathrm{Aff}(3,3)$. □

The case $p = 2$ can also be dealt with. By elementary arguments a primitive group of degree 8 is at least 2 - transitive (see for example Wielandt [11; page 49]). We have the following list of 7 examples and these are all (Burnside [5], page 218).

Group	Order	Transitivity	G_α
S_8	$2^7 \cdot 3^2 \cdot 5 \cdot 7 = 8!$	8	S_7
A_8	$2^6 \cdot 3^2 \cdot 5 \cdot 7 = \frac{1}{2} 8!$	6	A_7
Aff(3,2)	$8 \cdot 7 \cdot 6 \cdot 4$	3	GL(3,2)
PGL(2,7)	$8 \cdot 7 \cdot 6$	3	Aff(1,7)
PSL(2,7)	$8 \cdot 7 \cdot 3$	2	S Aff(1,7) = $\{x \to a^2x+b\}$
Aff(1,8)	$8 \cdot 7 \cdot 3$	2	$C_7 \rtimes C_3$
$\{x \to ax + b :$ $a \in \mathbb{F}_8 \setminus \{0\}$, $b \in \mathbb{F}_8\}$	$8 \cdot 7$	2	C_7

4.4 Groups Preserving Lines But Not Planes.

As noted in section 4.1 it is conceivable that there are groups G permuting Ω which permute some lines as lines but no planes. The proof of theorem 4.1 shows that if there are three lines through θ, λ_i, $i = 1,2,3$, such that λ_i^g is a line for all $g \in G$ and λ_i lies in the plane π for all i, then π^g is a plane for all $g \in G$. Thus the set S of theorem 4.1 has no three points collinear.

Suppose that there is a line in Λ as defined in section 4.1. Then for any orbit Δ on lines through θ and in Λ, ψ_Δ consists of lines through θ, no three in a plane. As noted before, this can happen only if the points where ψ_Δ intersects the plane at infinity form a k - arc in the sense of Dembowski [7; page 149] where k is the number of lines in ψ_Δ through θ. Thus $k \leq p+1$ if $p > 2$. Moreover by theorem 3.15, $k \geq 3$.

For λ_i, λ_j in ψ_Δ and through θ let π_{ij} be the plane spanned by λ_i and λ_j. Then as in the discussion after theorem 3.13, the function $f = \sum_{i<j} \chi_{\pi_{ij}}$ is in $F_1 G_\theta$ and $f \in C$ or $\deg f = p-1$. We will show that $f \notin C$. First by theorem 3.15, $3 \leq k$ and from above $k \leq p+1$. If $\rho_1 \in \psi_\Delta$ then $\rho_1 \, I \, \lambda_i$, say, and $\forall_{j \neq i} \chi_{\pi_{ij}}(\rho_1) = 1$, and since no three of the λ's are coplanar, $\chi_{\pi_{i'j}}(\rho_1) = 0$ if $i' \neq i$. Thus $f(\rho_1) = k-1$. However if $\rho_2 \notin \psi_\Delta$ then $\chi_{\pi_{ij}}(\rho_2) \neq 0$ only if ρ_2 happens to be in π_{ij}. Since there is at most one j, given an i, with $\pi_{ij} \, I \, \theta \cdot \rho_2$ there are at most $\frac{k}{2}$ planes π_{ij} with $\chi_{\pi_{ij}}(\rho_2) \neq 0$. Therefore $f(\rho_2) \leq \frac{k}{2}$. But since $3 \leq k \leq p+1$,

$\frac{k}{2} < k-1 \leq p$ and $f(\rho_1) \neq f(\rho_2)$.

Thus, when G preserves some lines there is a function f in $F_1 G_\theta$ of degree $p-1$. Hence we have a G - module $M = f * C^\perp$ of degree $p-2$. Therefore every function in M has integral zero over every line of Ω . Also M contains the partial derivatives of f .

Recall that $f = \frac{k(k-1)}{2} - \sum_{i<j} \pi_{ij}^{p-1}$. As we have observed there is a linear differential operator ∂_i for each λ_i such that $\partial_i(\pi) = 0$ if and only if $\lambda_i \; I \; \pi$. Since the degree of f is small we may differentiate without worry. Let $h = \partial_3 \partial_4 \ldots \partial_k f$. Then we have annihilated all terms π_{ij}^{p-1} with i or $j = 3,4,\ldots$, or k . Moreover we have not annihilated the π_{12}^{p-1} term since none of the lines $\lambda_3,\ldots,\lambda_k$ are in the plane π_{12} . Hence, there is a constant, a , such that $a \neq 0$ and $h = a\pi_{12}^{(p-1)-(k-2)}$.

Theorem 4.7: If there is a line λ of Ω which is mapped to a line by every element of G , but there is no plane which is always mapped to a plane, and if k is the number of lines in the G_θ - orbit of λ, then $\frac{p+3}{2} < k < p$.

Proof: If $k \leq \frac{p+3}{2}$ then $(p-1)-(k-2) \geq \frac{p-1}{2}$ and some derivative of h is of the form $a \cdot \pi_{12}^{(p-1)/2}$, $a \neq 0$, a constant. But then, by theorem 4.3, the zeros of $(\pi_{12}^{(p-1)/2})^g$ are a plane for each $g \in G$. Thus π_{12} is mapped to a plane by every g in G , a contradiction. □

Actually we have shown more. For if there is a G_θ - orbit with points from only k lines, where $4 \leq k \leq \frac{p+3}{2}$, then the argument given above yields at least 4 planes through θ which are always mapped to

planes by G, even without the assumption that there is a line which is always mapped to a line. Thus theorem 4.1 gives the following:

Theorem 4.8: If there is a G_θ - orbit with points from only k lines, where $4 \leq k \leq \frac{p+3}{2}$, then $G \leq \mathrm{Aff}(3,p)$.

CHAPTER V

Geometric Examples

In this section some examples will be given of some subgroups of $Aff(3,p)$ which illustrate various possibilities of earlier theorems.

5.1 $F_1\ G_\theta^o$ Trivial.

There is a theorem of Singer [13] which states that $PG(2,q)$ has, for each q, a transitive collineation, σ, of order q^2+q+1. By the fundamental theorem of classical projective geometry, σ comes from a matrix in $GL(3,q)$ which permutes the lines through θ in one long cycle and is regular on these lines. Thus (with $q=p$), we have a matrix $A \in GL(3,p)$ which permutes the points of $V(3,p)$ in orbits of length p^2+p+1, one point of each orbit on each line through θ. Therefore the group $T \rtimes \langle A \rangle$, the split extension of T by $\langle A \rangle$, is an example of a G with $F_1\ G_\theta^o$ trivial and each non-trivial G_θ-orbit has one point in common with each line through θ. By extending by appropriate subgroups of D, the dilations, we can have any divisor of $p-1$ as this number of common points. Moreover, by theorem 3.15, each of these G's is primitive.

Example 5.1: $p = 3$, $A = \begin{bmatrix} 0 & -1 & 0 \\ 0 & 1 & -1 \\ 1 & 0 & 1 \end{bmatrix}$, $G = T \rtimes \langle A \rangle$.

The function f of theorem 3.13 is $f = (XZ^2-XY^2-X^2Z+YZ^2) + (X-Y+Z)$. If Δ is one of the non-trivial orbits of G_θ then $\chi_\Delta = -1 \pm f + \chi_{\Omega-\theta}$.

Examples 5.2: $p = 5$. Let $A = \begin{pmatrix} 0 & -1 & 0 \\ 0 & -1 & -1 \\ 1 & 0 & -1 \end{pmatrix}$, $D_{-1} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ be matrices over $\mathbb{F}_5$.

With $G = T \rtimes \langle A \rangle$, G has rank 5 and the f of theorem 3.13 is a polynomial of degree 9 with terms of degrees 9, 5 and 1.

With $G = T \rtimes \langle A, D_{-1} \rangle$, we have a rank 3 group with each non-trivial G_θ orbit having 2 points on each line through θ . The new "f" is f^2 from above.

5.2 $F_1\, G_\theta^o$ Non-Trivial.

In this case there is more than one set, ψ_Δ , of lines through θ and a G_θ - orbit Δ . For $p = 3$ we have essentially only one geometric example and for $p = 5$ several.

Example 5.3: $p = 3$. Let $A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 & 0 \\ -1 & -1 & 0 \\ -1 & 0 & -1 \end{pmatrix}$ be matrices over $\mathbb{F}_3$. Then $G = T \rtimes G_\theta$ with $G_\theta = \langle A, B \rangle$ is a uni-primitive group acting on $V(3,3)$. It has G_θ - orbits of length 1, 6, 8, 12. These cover 3, 4 and 6 lines through θ , respectively. If we intersect these G_θ line-orbits with the plane at infinity we obtain the following three sets: a conic, its exterior points (points on two tangents of the conic) and its interior points (points on no tangent). This is the only possible configuration .

Since G has rank 4, $\dim_{\mathbb{F}_3}(F_1\, G_\theta) = 4$. The orbits of G_θ are

$$\Delta_0 = \{(0,0,0)\}$$

$$\Delta_1 = \{\pm(0,1,1), \pm(1,-1,0), \pm(1,0,-1)\}$$

$$\Delta_2 = \{\pm(1,0,0), \pm(0,1,0), \pm(0,0,1), \pm(1,-1,-1)\}$$

$$\Delta_3 = \{\pm(1,1,-1), \pm(1,-1,1), \pm(1,1,1), \pm(1,1,0), \pm(1,0,1), \pm(0,1,-1)\} .$$

$$\chi_{\Omega\setminus\theta} = 1+(X^2-1)(Y^2-1)(Z^2-1) = X^2Y^2Z^2 - (X^2Y^2+X^2Z^2+Y^2Z^2)+X^2+Y^2+Z^2$$

$$-\chi_{\Delta_1} = (X^2Y^2+X^2Z^2+Y^2Z^2) + (-X^2YZ+XY^2Z+XYZ^2) + (-XY-XZ+YZ)$$

$$-\chi_{\Delta_2} = -X^2Y^2Z^2 - (X^2Y^2+X^2Z^2+Y^2Z^2) + (-X^2YZ+XY^2Z+XYZ^2) - (X^2+Y^2+Z^2) .$$

Thus $\chi_{\Delta_3} = -(X^2Y^2+X^2Z^2+Y^2Z^2) - (X^2YZ+XY^2Z+XYZ^2) + (-XY-XZ+YZ)$. Moreover $\chi_{\Omega-\theta} - \psi_{\Delta_2} + \psi_{\Delta_1} = XY + XZ - YZ$. Therefore

$$F_1 G_\theta = (F_1 G_\theta^o) = \langle 1\rangle \oplus \langle XY+XZ-YZ\rangle \oplus \langle \chi_{\Delta_1}\rangle \oplus \langle \chi_{\Omega-\theta}\rangle .$$

degrees: 0 2 4 6

There is an example with the same line orbits but with Δ_2 split into 2 sets of four points.

Example 5.4: $p = 5$. Let the following be matrices over $\mathbb{F}_5$:

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} , \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} , \quad C = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} , \quad E_{s,t} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & t \\ 0 & s & 0 \end{pmatrix}$$

$$L = \begin{pmatrix} 1 & -2 & -2 \\ -2 & 1 & -2 \\ -2 & -2 & 1 \end{pmatrix} , \quad D_{-1} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} .$$

Let $G = T \rtimes G_\theta$.

(i) Let $G_\theta = \langle A,B,C\rangle$. Then G_θ has orbits touching 3, 4, 6, 6 and 12 lines, respectively, through θ . G acts on the set of 3 lines as C_3 . These lines fall into 9 point orbits

(not counting θ itself) as follows; 6, 6; 8, 8; 24; 12, 12; 24, 24.

(ii) Let $G_\theta = \langle A,B,C,E_{1,-1}\rangle$. Then G_θ has the same line orbits but acts on the one of length 3 as S_3 .

(iii) With $G_\theta = \langle A,B,C,E_{1,2}\rangle$, G_θ has 3 orbits of lines through θ , of lengths 3, 12 and 16. The configuration which they make on π_∞ is the 3 points of a triangle, the 12 remaining points on the sides of the triangle, and the points not on any side.

(iv) If $G_\theta = \langle A,B,C,L\rangle$ then G has 3 orbits of lines again but this time they have lengths 6, 10 and 15. Their images on π_∞ consist of a conic, its exterior points and its interior points. The conic is $X^2 + Y^2 + Z^2 = 0$. G_θ is 2 - transitive on the orbit of 6 lines.

BIBLIOGRAPHY

[1] A. Albert, and R. Sandler, "An Introduction to Finite Projective Planes". New York, Holt, Rinehart and Winston, 1968.

[2] E. Artin, "Geometric Algebra". New York, Interscience Publishers Inc., 1957.

[3] H.F. Baker, "A Locus with 25,920 Linear Self-transformations". Cambridge tracts in Mathematics and Mathematical Physics, No. 39; Cambridge, University Press, 1946.

[4] N. Biggs, "Finite Groups of Automorphisms". London Mathematical Society Lecture Note Series, 6; Cambridge University Press, 1971.

[5] W. Burnside, "Theory of Groups of Finite Order". New York, Dover Publications Inc., 1955.

[6] P. Dembowski, "Finite Geometries". Berlin, Springer-Verlag, 1968.

[7] L.E. Dickson, "Linear Groups with an Exposition of the Galois Field Theory". New York, Dover Publications, Inc. 1958.

[8] D.G. Higman, "Finite Permutation Groups of Rank 3". Math. Z. 86 (1964) 145-156.

[9] J. Singer, "A Theorem of Projective Geometry and Some Applications to Number Theory". Trans. Amer. Math. Soc. 43(1938), 377-385.

[10] H. Wielandt, "Finite Permutation Groups". New York, Academic Press, 1964.

[11] H. Wielandt, "Permutation Groups through Invariant Relations and Invariant Functions". Columbus, Ohio, Department of Mathematics, The Ohio State University, 1969.